การใช้งาน Endian Firewall Community 2.3 : ตอน การเซ็ตอัพเครือข่าย

แปลโดยอดิศร ขาวสังข์

จัดทำเมื่อ 11 มกราคม 2553

Endian Firewall Community เป็น linux security distribution ที่มีฟังก์ชันของระบบการจัดการความปลอดภัยทางเครือข่ายแบบรวม (UTM : Unified Threat Management) เป็นซอฟต์แวร์ที่ได้ออกแบบมาเพื่อให้จัดการและใช้งานได้ง่าย โดยมีคุณสมบัติที่ประกอบด้วย Stateful Packet Inspection (SPI) Firewall แอพพลิเคชันพร๊อกซี่สำหรับ HTTP,FTP, POP3,SMTP และ DNS เครื่องมือในการกลั่นกรองเว็บรวมถึง VPN แบบ OpenVPN และ IPSec โดยข้อดีหลักของ Endian Firewall Community คือเป็น Open Source ที่สามารถประยุกต์ใช้งานกับเครือของเราได้ฟรี

ความสามารถที่ทางเว็บไซต์ของ EFW (http://www.efw.it) แจ้งไว้มีดังนี้

- การสำรองข้อมูล

  สามารถบันทึกและกู้คืนผ่าน USB device สามารถตั้งเวลาให้มีการสำรองข้อมูลแบบอัตโนมัติและส่งข้อมูลการสำรองที่ผ่านการเข้ารหัสแล้วผ่านทางอีเมล์

- **Dashboard**

  หน้าเพจหลักจะถูกแทนที่ด้วย dashboard ซึ่งเป็นสถิติเกี่ยวกับระบบและบริการต่างๆ อันเป็นกราฟแบบ live-graphs สำหรับทราฟฟิกขาเข้าและขาออก

- **ระบบแจ้งเตือนทางอีเมล์**

  เป็นการส่งอีเมล์โดยอัตโนมัติตามที่ได้กำหนด เมื่อมีเหตุการณ์ต่างๆ เกิดขึ้น

- **HTTP proxy time based access control**

  เป็นการควบคุมการเข้าใช้งาน HTTP Proxy โดยกำหนดช่วงเวลาในการใช้งานได้

- **HTTP proxy with user- and group-based content filtering**

  เป็นความสามารถในการกำหนดผู้ใช้งานและกลุ่มผู้ใช้งานเพื่อควบคุมการกลั่นกรองการเข้าใช้งานเว็บไซต์

- **Intrusion Prevention**

  มีระบบการการป้องการการบุกรุกทางเครือข่ายโดยใช้กฎของ Snort ที่สามารถคอนฟิกได้ ซึ่งสามารถที่จะละทิ้งแพ็กเกตการบุกรุกที่เหมือนกับข้อมูลใน Log ได้

- **Policy routing**

  สามารถสร้างกฎการจัดเส้นทางโดยยึดถืออินเตอร์เฟส, MAC Address หรือพอร์ตของแพ็กเกตได้

- **Port forwarding rewrite**

  การทำ Porwarding ในเวอร์ชันก่อน 2.3 สามารถฟอร์เวิร์ดได้เฉพาะ Red zone เท่านั้น แต่ในเวอร์ชันนี้สามารถทำได้จากทุกโซนโดยปราศจากการทำ NAT

- **Quality of Service and Bandwidth Management**

  การจัดรูปร่างของทราฟฟิก (Traffic Shaping) ได้ถูกแทนที่ด้วย QoS Module ซึ่งสามารถทำได้โดยใช้ device, classes และ rules

- **SNMP support**

  สนับสนุน SNMP แบบพื้นฐาน ซึ่งการใช้งานต้องทำการ Enable SNMP Server พร้อมป้อนค่าที่เกี่ยวข้อง

- **SMTP proxy web interface rewrite**

  ได้มีการปรับปรุง Web Interface ในส่วน SMTP Proxy โดยเน้นการใช้งานที่สะดวก

- **VLAN support (IEEE 802.1Q trunking)**

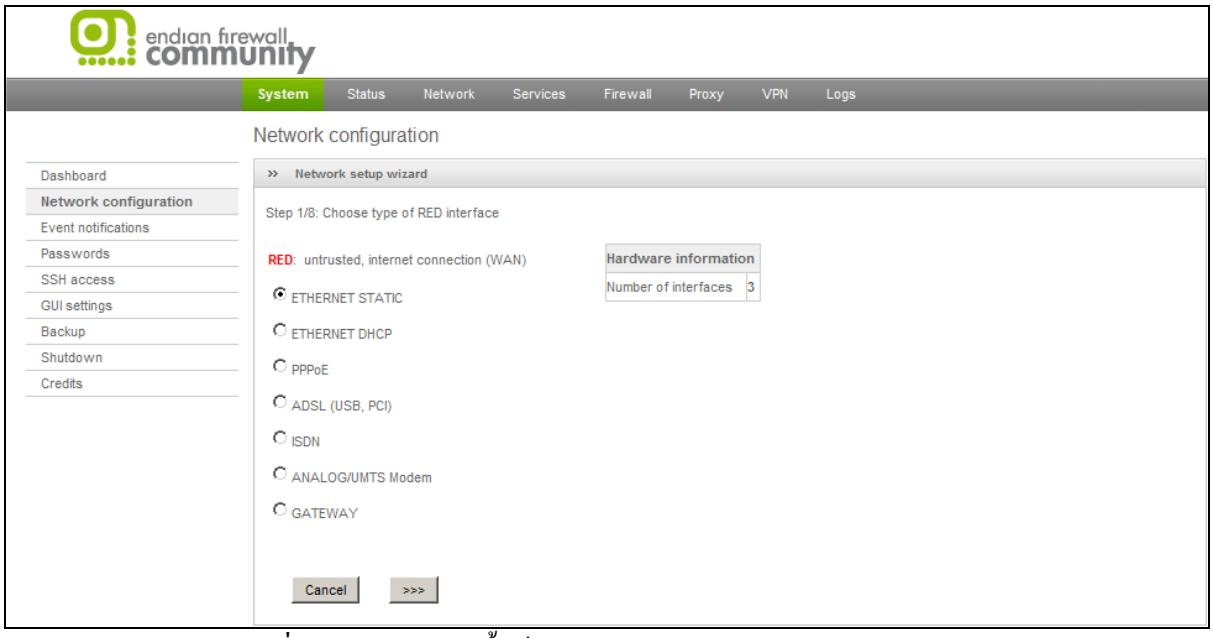
  เวอร์ชันนี้สามารถสร้าง VLANs บนทุก Interface ได้ โดย VLAN Interface สามารถใช้งานเพื่อแบ่งแยกการเชื่อมต่อในโซนเดียวกัน

การเซ็ตอัพเครือข่าย

ทำได้ด้วยเลือกเมนู System จาก Menu bar ส่วนบนของหน้าจอ แล้วเลือกเมนูย่อย Network configuration ทางด้านซ้ายของหน้าจอ

การเลือกชนิดของ Red Interface

เมื่อเราติดตั้ง Endian Firewall Community แล้ว อินเตอร์เฟสที่เป็น trusted network (เรียกว่า Green Interface) จะถูกเลือกและเซ็ตอัพ และการเลือก untrusted interface network (เรียกว่า Red Interface) เพื่อเชื่อมต่อไปยังผู้ให้บริการอินเตอร์เน็ต (outside) สามารถใช้งานได้เป็น 7 รูปแบบดังนี้



รูปที่ 1 แสดงรูปแบบทั้งเจ็ดของการเลือกชนิดของ RED Interface

1. **ETHERNET STATIC**

ต้องมีการเซ็ตอัพค่าข้อมูลเครือข่ายของ Ethernet Adapter เช่น IP และ Netmask เป็นแบบ manual การใช้งานแบบนี้โดยทั่วไปจะเชื่อมต่อ RED Interface กับเราเตอร์โดยใช้สายอีเทอร์เน็ต แบบ crossover

2. **ETHERNET DHCP**

เป็นการเซ็ตอัพค่าข้อมูลเครือข่ายของ Ethernet Adapter ให้รับค่าจาก DHCP การใช้งานแบบนี้ใช้สำหรับการเชื่อมต่อ RED Interface กับ cable modem/router หรือ ADSL/ISDN router โดยใช้สายอีเทอร์เน็ตแบบ crossover

3. **PPPoE**

เป็นการเชื่อมต่อ Ethernet adapter แบบ crossover เข้ากับ ADSL modem การใช้งานแบบนี้ต้องเซ็ตค่าที่โมเด็มเป็นแบบบริดจ์ และให้เครื่องที่เป็น EFW Community ใช้ PPPoE เชื่อมต่อกับผู้ให้บริการ ทั้งนี้อย่าสับสนกับการใช้งานผ่าน ADSL modem ที่เป็นแบบ ETHERNET STATIC และ ETHERNET DHCP ซึ่งทั้งสองแบบนี้มีการทำ PPPoE บนตัว Router เอง

4. **ADSL (USB, PCI)**

เป็นการใช้งานกับ ADSL modem แบบ USB และ PCI

5. **ISDN**

เป็นการใช้งานกับ ISDN adapter

6. **ANALOG/UMTS Modem**

เป็นการใช้งานกับระบบอานาล็อก (dial-up) หรือ UMTS (cell-phone) modem

7. **GATEWAY**

เป็นการใช้งานกับเครื่องที่ไม่มี RED Interface การใช้งาน Firewall โดยทั่วไปจะต้องมีสองอินเตอร์เฟสเป็นอย่างน้อย แต่บางสถานการณ์เราสามารถใช้แค่อินเตอร์เฟสเดียวได้ เช่น การใช้งานที่ต้องการทำเป็น Firewall อย่างเดียวเท่านั้น หรืออีกแบบอาจจะใช้ในกรณีที่ BLUE zone ของ EFW ถูกเชื่อมต่อกับ VPN ผ่าน GREEN interface ของ EFW ตัวที่สอง ในสถานการณ์แบบนี้ IP Address ของ Green interface ของ Firewall ตัวที่สอง สามารถถูกใช้เป็น backup uplink บน Firewall ตัวแรก ซึ่งถ้าเลือกออฟชันนี้จะต้องมีการคอนฟิก default gateway ในภายหลัง